CLAIMS

What is claimed is:

1. In a network device having a plurality of ports and providing routing functionality between ports, a method for providing security, comprising:

identifying at least a first port of a the network device, having a first gateway address, as being a management port;

identifying a group of ports of the network device as being a non-management ports; and

filtering out management data packets received on any of the non-management ports.

2. The method of claim 1, further wherein the filtering out management data packets includes:

determining if a destination IP address for a data packet received on one of the group of non-management ports has a destination IP address which corresponds to the gateway address of the first port.

3. The method of claim 2, wherein the filtering out management data packets includes:

determining if a data packet received on one of the group of ports utilizes a management protocol; and

dropping a data packet where it is determined that a data packet received on one of the group of ports has a destination IP address which corresponds to the gateway address of the first port, and that the data packet utilizes a management protocol.

4. The method of claim 1, further comprising:

defining a virtual local area network to include the first port, and to include a first layer 2 subnet;

allowing access to management functions of the network device only to those hosts which are connected to the first layer 2 subnet.

5. The method of claim 1, further comprising:

defining a virtual local area network to include the first port, and to include a first layer 2 subnet;

allowing access to management functions of the network device only to those hosts which are connected to the first layer 2 subnet;

connecting a first layer 2 switch to a second port of the group of ports;

defining a plane of the layer 2 device to be part of the virtual local area network, wherein the plane of the layer 2 device is assigned a source IP address which corresponds to the gateway address of the first port; and

and wherein all management for the first layer 2 device are sent to the source IP address which is assigned to the plane of the layer 2 device is part of the virtual local area network.

6. The method of claim 5, wherein all management commands have higher priority than all other data packets routed through the network device.

7. The method of claim 1, further including:

providing an application specific integrated circuit which is operable to filter out all management data packets received on any of the non-management ports.

8. The method of claim 1 further including:

providing an application specific integrated circuit which is operable to determine if a destination IP address for a data packet received on one of the group of non-management ports is a destination IP address which corresponds to the gateway address of the first port, and to determine if a data packet received on one of the first group of ports utilizes a management protocol, and to drop a data packet where it is determined that a data packet received on one of the group of ports has a destination

IP address which corresponds to the gateway address of the first port, and that the data packet utilizes a management protocol.

9. A network device for routing data packets, the network device including:

a first port which is defined to be a management port;

a group of ports which are not management ports;

a CPU which is operable to provide management functions, which allow a user to modify the operation of the network device;

an application specific integrated circuit which is operable to deny access to the CPU management functions for all hosts which transmit data packets to the network device through any of the group of ports.

10. The network device of claim 9, wherein:

the first port has a first gateway IP address;

wherein the application specific integrated circuit receives data packets, received on each port of the group of ports, and is operable to determine if a data packet received on one the group of ports contains a destination IP address which corresponds to the first gateway IP address;

wherein the application specific integrated circuit is further operable to determine if a data packet received on one of the group of ports utilizes a management protocol; and

wherein when it is determined that a data packet received on one of the group of ports is directed to a destination IP address which corresponds to the first gateway IP address and is in a management protocol, the application specific integrated circuit operates to drop the data packet.

11. The network device of claim 10, wherein the first port is defined to be part of a management virtual local area network, and only devices are coupled to the management virtual area network have access to the management functions of the CPU.